UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/517,335	02/28/2006	Bulent Ozgur Gurleyen	P08623US00 / BAS	2759

881 7590 09/08/2009

STITES & HARBISON PLLC
1199 NORTH FAIRFAX STREET
SUITE 900
ALEXANDRIA, VA 22314

EXAMINER	
WRIGHT, BRYAN F	

ART UNIT	PAPER NUMBER
2431	

MAIL DATE	DELIVERY MODE
09/08/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Advisory Action Before the Filing of an Appeal Brief	Application No.	Applicant(s)	
	10/517,335	GURLEYEN ET AL.	
	Examiner	Art Unit	
	BRYAN WRIGHT	2431	

--The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

THE REPLY FILED 26 August 2009 FAILS TO PLACE THIS APPLICATION IN CONDITION FOR ALLOWANCE.

1. ☒ The reply was filed after a final rejection, but prior to or on the same day as filing a Notice of Appeal. To avoid abandonment of this application, applicant must timely file one of the following replies: (1) an amendment, affidavit, or other evidence, which places the application in condition for allowance; (2) a Notice of Appeal (with appeal fee) in compliance with 37 CFR 41.31; or (3) a Request for Continued Examination (RCE) in compliance with 37 CFR 1.114. The reply must be filed within one of the following time periods:

a) ☐ The period for reply expires _____months from the mailing date of the final rejection.

b) ☒ The period for reply expires on: (1) the mailing date of this Advisory Action, or (2) the date set forth in the final rejection, whichever is later. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of the final rejection.

Examiner Note: If box 1 is checked, check either box (a) or (b). ONLY CHECK BOX (b) WHEN THE FIRST REPLY WAS FILED WITHIN TWO MONTHS OF THE FINAL REJECTION. See MPEP 706.07(f).

Extensions of time may be obtained under 37 CFR 1.136(a). The date on which the petition under 37 CFR 1.136(a) and the appropriate extension fee have been filed is the date for purposes of determining the period of extension and the corresponding amount of the fee. The appropriate extension fee under 37 CFR 1.17(a) is calculated from: (1) the expiration date of the shortened statutory period for reply originally set in the final Office action; or (2) as set forth in (b) above, if checked. Any reply received by the Office later than three months after the mailing date of the final rejection, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

NOTICE OF APPEAL

2. ☐ The Notice of Appeal was filed on _____. A brief in compliance with 37 CFR 41.37 must be filed within two months of the date of filing the Notice of Appeal (37 CFR 41.37(a)), or any extension thereof (37 CFR 41.37(e)), to avoid dismissal of the appeal. Since a Notice of Appeal has been filed, any reply must be filed within the time period set forth in 37 CFR 41.37(a).

AMENDMENTS

3. ☐ The proposed amendment(s) filed after a final rejection, but prior to the date of filing a brief, will not be entered because
   (a) ☐ They raise new issues that would require further consideration and/or search (see NOTE below);
   (b) ☐ They raise the issue of new matter (see NOTE below);
   (c) ☐ They are not deemed to place the application in better form for appeal by materially reducing or simplifying the issues for appeal; and/or
   (d) ☐ They present additional claims without canceling a corresponding number of finally rejected claims.

   NOTE: _____. (See 37 CFR 1.116 and 41.33(a)).

4. ☐ The amendments are not in compliance with 37 CFR 1.121. See attached Notice of Non-Compliant Amendment (PTOL-324).

5. ☐ Applicant's reply has overcome the following rejection(s): _____.

6. ☐ Newly proposed or amended claim(s) _____ would be allowable if submitted in a separate, timely filed amendment canceling the non-allowable claim(s).

7. ☒ For purposes of appeal, the proposed amendment(s): a) ☐ will not be entered, or b) ☒ will be entered and an explanation of how the new or amended claims would be rejected is provided below or appended.
   The status of the claim(s) is (or will be) as follows:
   Claim(s) allowed: _____.
   Claim(s) objected to: _____.
   Claim(s) rejected: *30-58*.
   Claim(s) withdrawn from consideration: _____.

AFFIDAVIT OR OTHER EVIDENCE

8. ☐ The affidavit or other evidence filed after a final action, but before or on the date of filing a Notice of Appeal will not be entered because applicant failed to provide a showing of good and sufficient reasons why the affidavit or other evidence is necessary and was not earlier presented. See 37 CFR 1.116(e).

9. ☐ The affidavit or other evidence filed after the date of filing a Notice of Appeal, but prior to the date of filing a brief, will not be entered because the affidavit or other evidence failed to overcome all rejections under appeal and/or appellant fails to provide a showing a good and sufficient reasons why it is necessary and was not earlier presented. See 37 CFR 41.33(d)(1).

10. ☐ The affidavit or other evidence is entered. An explanation of the status of the claims after entry is below or attached.

REQUEST FOR RECONSIDERATION/OTHER

11. ☒ The request for reconsideration has been considered but does NOT place the application in condition for allowance because: See Notes 1 & 2 Below:.

12. ☐ Note the attached Information *Disclosure Statement*(s). (PTO/SB/08) Paper No(s). _____

13. ☐ Other: _____.

/William R. Korzuch/
Supervisory Patent Examiner, Art Unit 2431

/BRYAN WRIGHT/
Examiner, Art Unit 2431

Note: The Examiner contends paragraph 21 and 24 are the only paragraphs in applicant's original disclosure which define "security data" and the usage of "security data" in regards to the claim invention. Paragraph 21 and 24 reads:

[0021] In a PSD one device has the role of a PSD administrator. This device includes security data (for example a shared key or a public-private key pair) that can be selectively passed to other devices that are to join the PSD. Communication can only successfully occur between devices that have this security data. Once a device has the security data, it can communicate with other devices in the PSD without referring to the PSD administrator…

Description of Disclosure - DETX (22):
[0024] One device within the PSD is nominated as the PSD administrator. The PSD administrator is a role that could be assumed by any of the devices in the PSD provided it contains the necessary hardware to support the role, for example a secure key store and/or a display. The administrator role may be moved from one device to another. If the administrator role is moved to a new device, the new device will have passed thereto, or have pre-stored thereon, the necessary security data to allow the admission of new devices to the PSD.

Applicant filed an amendment on 11/26/2008, adding the following subject matter of: "including security data for identifying each device as a member of the domain and device identity data corresponding to each member of the domain, said device identity data being required to allow each device in the domain to establish secure communications directly with each other device within the domain". The Examiner contends that applicant's original specification does not support applicant's claim element of the "security data" used for identifying each device as a member nor does the original disclosure support the claim element of a "device identity data" required to allow each device in the domain to communicate. As recited in applicant's paragraph 21, it is the "security data" that establishes communication, not the "device identity data" as asserted in the claim language.

Applicant's remarks presented on 8/26/2009 alleges deficiency on the part of Elson in view of Gehrmann based on the new matter presented on 11/26/2008 of: "including security data for identifying each device as a member of the domain and device identity data corresponding to each member of the domain, said device identity data being required to allow each device in the domain to establish secure communications directly with each other device within the domain".

The Examiner contends that Elson in view of Gehrmann teaches the use of "security data" (e.g., shared key or a public-private key pair) to facilitate communication as formally presented in applicant's original disclosure [par. 21]. The Examiner respectfully draws applicant's attention to Ghermann pg 2, lines 15-30 in which Ghermann discloses X.509 certificate. The X.509 certificate includes a public key, and the name (e.g., identification) of the subject associated with the public key. This certificate is digitally signed. When the signature is verified communication is established. In this instance the certificate would be equivalent to applicant's "security data". Secondly, Ghermann also discloses session key (e.g., group key) and the use of PKI to distribute the session keys in the "Description of Related Art". Session keys are commonly shared between group members to establish communication link between communicating entities. Further, Ghermann discloses the use of PKI a bases in ad hoc communication networks (e.g. PAN) pg. 4, lines 15-20. In this instance the PKI in combination with session key (e.g., group key) distribution would be equivalent to applicant's "security data".

Furthermore, in view of applicants new matter assertion of "including security data identifying a device" presented 11/26/2008, the Examiner respectfully submits the X.509 certificate which Gehrmann discloses contains the identity of the device associated to the public key certificate and could be used to identify the group member. In this instance the certificate is equivalent to applicant's "security data" as claimed. Additionally, the Examiner contends Ghermann discloses maintaining a list of each node [pg. 9, lines 15-20] for the purpose of member authentication. Once the group member is authenticated the group member can begin communicating. In this instance the list could be interpreted by those of ordinary skill in the art as "security data" because the list contains the identification of all group members and is used to specifically authenticate a group member. Subsequently, Ghermann's disclosure of said list yields equivalency to applicant's new matter assertion of "device identity data" required to allow each device in the domain to establish secure communication. Again the list maintains group members (i.e., member identification) for the purpose of facilitating group communication.

Note 2: With regards to applicant's remarks questioning the motivation to combine Elson and Gehrmann, the Examiner contends Elson discloses dynamic networking between multiple devices for the purpose of sharing information [fig. 34]. In Elson, devices communicate with each other as prescribed by policy and protocol data. Gehrmann teaches an "ad hoc" network where members communicate with one another [fig. 1]. Members join and leave. Both Elson and Gehrmann disclose a dynamic network of communicating devices for the purpose of sharing data. Modifying Elson with Gehrmann, one would appreciate an enhancement in communication security between the existing network communicating group members and joining members.